SYSTEM AND METHOD OF USING THE PUBLIC SWITCHED TELEPHONE NETWORK IN PROVIDING AUTHENTICATION OR AUTHORIZATION FOR ONLINE TRANSACTIONS

The benefit of a December 15, 1999 filing date for Provisional Patent Application Ser. No. 60/170,808 is hereby claimed.

Field of the Invention

This invention relates generally to Internet security. More particularly, this invention relates to the method of attempting to verify the identity of an Internet user.

Background of Invention

The internet offers the prospect of expanded, world-wide commerce, e-commerce, with potentially lower cost to purchasers than heretofore possible. However, the lack of direct person-to-person contact has created its own set of problems. Identity theft is a problem threatening the growth of e-commerce.

E-commerce growth will only occur if there is a trusted and reliable security infrastructure in place. It is imperative that the identity of site visitors be verified before granting them access to any online application that requires trust and security. According to the National Fraud Center, its study of identity theft "led it to the inescapable conclusion that the only realistic broad-based solution to identity theft is through authentication." *Identity Theft: Authentication As A Solution, page 10, nationalfraud.com.*

In order to "authenticate" an entity, one must:

1) identify the entity as a "known" entity;
2) verify that the identity being asserted by the entity is its true identity; and,
3) provide an audit trail, which memorializes the reasons for trusting the identity of the entity.

In the physical world, much of the perceived security of systems relies on physical presence. Traditionally, in order to open a bank account, an applicant must physically appear at a bank branch, assert an identity, fill out forms, provide signatures on signature cards, etc. It is customary for the bank to request of the applicant that they provide one or more forms of identification. This is the bank's way of verifying the applicant's asserted identity. If the bank accepts, for instance, a driver's license in

accepting as a form of identification, then the bank is actually relying on the processing integrity of the systems of the state agency that issued the driver's license that the applicant is who he/she has asserted themselves to be.

The audit trail that the bank maintains includes all of the forms that may have been filled out (including signature cards), copies of important documents (such as the driver's license), and perhaps a photo taken for identification purposes. This process highlights the reliance that a trusted identification and authentication process has on physical presence.

In the electronic world, the scenario would be much different. An applicant would appear at the registration web site for the bank, enter information asserting an identity and click a button to continue the process. With this type of registration, the only audit trail the bank would have is that an entity from a certain IP address appeared at the web site and entered certain information. The entity may actually have been an automated device. The IP address that initiated the transaction is most likely a dynamically-assigned address that was issued from a pool of available addresses. In short, the bank really has no assurance of the true identity of the entity that registered for the account.

To resolve this issue, many providers of electronic commerce sites have begun to rely on mechanisms that do not happen as part of the actual electronic transaction to help provide assurance that the transaction is authentic. These mechanisms are generally referred to as "out-of-band" mechanisms. The most frequently used out-of-band authentication mechanism is sending the end user a piece of mail via the United States Postal Service or other similar delivery services. The piece of mail sent to the end user will contain some piece of information that the site requires the end user to possess before proceeding with the registration.

By sending something (e.g.,., a PIN number) through the mail, and then requiring the end user to utilize that piece of information to "continue" on the web site, the provider of the site is relying on the deterrent effects of being forced to receive a piece of mail at a location, including but not limited to, the federal laws that are intended to prevent mail fraud. The primary drawback of using the mail is that it is slow. In

addition, there is no audit trail. In this day and age of the Internet, waiting "7-10 days" for a mail package to arrive is not ideal for the consumer or the e-commerce site.

An authentication factor is anything that can be used to verify that someone is who he or she purports to be. Authentication factors are generally grouped into three general categories: something you know, something you have, and something you are.

A "something you know" is a piece of information which alone, or taken in combination with other pieces of information, should be known only by the entity in question or those whom the entity in question should trust. Examples are a password, mother's maiden name, account number, PIN, etc. This type of authentication factor is also referred to as a "shared secret".

A shared secret is only effective if it is maintained in a confidential fashion. Unfortunately, shared secrets are often too easy to determine. First, the shared secret is too often derived from information that is relatively broadly available (Social Security Number, account number). Second, it is difficult for a human being to maintain a secret that someone else really wants. If someone really wants information from you, they may go to great lengths to get it, either by asking you or those around you, directly or indirectly, or by determining the information from others that may know it.

A "something you have" is any physical token which supports the premise of an entity's identity. Examples are keys, swipe cards, and smart cards. Physical tokens generally require some out-of-band mechanism to actually deliver the token. Usually, some type of physical presence is necessary (e.g., an employee appearing in the human resources office to pick up and sign for keys to the building.)

Physical tokens provide the added benefit of not being "socially engineer-able", meaning that without the physical token, any amount of information known to a disreputable party is of no use without the token. A trusted party must issue the token in a trusted manner.

A "something you are" is some feature of a person that can be measured and used to uniquely identify an individual within a population. Examples are fingerprints, retina patterns, and voiceprints. Biometric capabilities offer the greatest form of identity authentication available. They require some type of physical presence and they are able to depict unique characteristics of a person that are exceedingly difficult to spoof.

Unfortunately, biometric devices are not yet totally reliable, and the hardware to support biometrics is expensive and not yet broadly deployed. Some biometric technology in use today also relies on an electronic "image" of the biometric to compare against. If this electronic image is ever compromised, then the use of that biometric as identity becomes compromised. This becomes a serious problem based on the limited number of biometrics available today. More importantly, biometrics cannot be utilized to determine an individual's identity in the first instance.

A security infrastructure is only as strong as its underlying trust model. For example, a security infrastructure premised upon security credentials can only address the problems of fraud and identity theft if the security credentials are initially distributed to the correct persons.

First-time registration and the initial issuance of security credentials, therefore, are the crux of any security infrastructure; without a trusted tool for initially verifying identity, a security infrastructure completely fails. The National Fraud Center explicitly noted this problem at page 9 of its report:

"There are various levels of security used to protect the identities of the [security credential] owners. However, the known security limitation is the process utilized to determine that the person obtaining the [security credential] is truly that person. The only known means of making this determination is through the process of authentication."

In any security model, the distribution of security credentials faces the same problem: how to verify a person's identity over the anonymous Internet. There are three known methods for attempting to verify a site visitor's identity. The three current methods are summarized below:

- Solution A: an organization requires the physical presence of a user for authentication. While the user is present, a physical biometric could be collected for later use (fingerprint, voice sample, etc.). The problem with the physical presence model is that it is extremely difficult and costly for a company to require that all of its employees, partners, and customers present themselves physically in

order to receive an electronic security credential. This model gets more difficult and more expensive as it scales to a large number of users.

- Solution B: a company identifies and authenticates an individual based on a shared secret that the two parties have previously agreed upon. The problem with the shared secret model is that it in itself creates a serious security problem: shared secrets can easily be compromised. Since the shared secret is relatively easy to obtain, this security model suffers from serious fraud rates. Use of an electronic copy of a specific biometric like a thumbprint could be used as a shared secret. But once it is compromised, one cannot reissue a new thumbprint and there is a limited set of others to choose from.
- Solution C: a company relies on communication of a shared secret through the postal service. This process begins when the user registers at a web site and enters uniquely identifying information. A personal identification number (PIN) is then sent to the user at a postal mailing address (assuming the identifying information is correct). The user must receive the PIN in the mail, return to the web site and re-register to enter the PIN. The postal service is used because it is a trusted network; there is some assurance of delivery to the expected party and there are legal implications for breach of the network. A large flaw with this method is the built-in delay of days, even weeks, before the user receives the PIN. This mode of authentication is too slow by today's business standards; the potential of the Internet to transform the structure of commerce rests firmly on the ability to process transactions rapidly. Too many people simply never finish the process. Moreover, there is a limited audit trail to refer to in the event of a dispute regarding the use of the security credential. A signature (another type of biometric) could be required, but that triples the delay until the PIN is returned. Organizations are seeing large number of potential customers not returning to close a transaction after these delays.

Table I summarizes characteristics of the known authentication processes.

	Authentication Processes		
Characteristics	***Physical Presence***	***Mail***	***Shared Secrets***
Automated			✔
Easily Scalable		✔	✔
Auditable	✔	✔	
Can use biometrics	✔		
Has legal protections	✔	✔	
Occurs in real time, therefore tends to retain customers			✔
Deters fraud	✔	✔	
Protects private data	✔		

TABLE I

Known solutions do not enable organizations to distribute efficiently and securely electronic security credentials. There continues to be a need for improved authentication or authorizing methods. Preferably such improvements could be realized without creating substantial additional complexity for a visitor to a site. It would also be preferable if such methods did not slow down the pace of the interaction or transaction.

Summary of the Invention

An automated system uses a publicly available communications network, such as the Public Switched Telephone Network (PSTN), wire line or wireless, to provide a real-time, interactive and largely self-service mechanism to aide in authentication (identity verification) and authorization (acceptance by a verified identity) for electronic transactions. Actions are coordinated between an electronic network (the Internet) and the Public Switched Telephone Network.

This coordination of an active Internet session with an active PSTN session can be used as a tool for verification. In one embodiment, it can be used to create an audit trait for any individual electronic transaction. These transactions may be, for example, the first-time issuance of an electronic security credential (e.g., passwords, digital

certificates, PINs) or the verification of a security credential already issued. Other transactions, without limitation, come within the spirit and scope of the present invention.

A visitor who has logged onto a site to obtain goods, services, credentials, access or the like, all without limitation, is requested to enter or to specify a telephone number where he/she can be contacted during the current session (multi-line environment), or between segments of the present session (single line environment). Authentication/authorization software can at this time transmit specific confirmation information to the user's display. This is information available only to the transmitting software and the recipient.

The authentication/authorization software then places a call, via the public switched telephone network, to the site visitor. The site visitor, on receipt of the call from the software, is requested to key in via phone pad or to read back the confirmation information via the telephone network. If will be understood that the order and timing of the presentation and capture of confirmation information can be varied based on the application.

This "out of band" confirmation has the advantage that the confirmation information is delivered to the visitor immediately while on-line. In a multi-line environment, the visitor stays on-line and receives an automated phone call, at the identified phone number essentially immediately. The visitor provides immediate confirmation information feedback, to the software.

In addition to the confirmation information, the software can initiate a voice based exchange, with the user. This exchange can be stored to provide an audit trail. The same audit trail can include the called telephone number, the non-verbal confirmation information and/or any additional transaction related information.

Once the software has authenticated or authorized the visitor, the visitor can be transferred, with appropriate authorization or access indicia to transaction or access providing software.

In one embodiment, the coordination of an active Internet session with an active PSTN session implements a method for providing real-time, fully-automated, two-factor authentication of an Internet user. This invention is an improvement over the known

process for helping to verify an Internet user's identity. The invention has benefits, illustrated in Table II, when compared to known processes:

	Authentication Processes			
Characteristics	***Telephone***	***Physical Presence***	***Mail***	***Shared Secrets***
Automated	✔			✔
Easily Scalable	✔		✔	✔
Auditable	✔	✔	✔	
Can use biometrics	✔	✔		
Has legal protection	✔	✔	✔	
Occurs in real time, therefore tends to retain customers	✔			✔
Deters fraud	✔	✔	✔	
Protects private data	✔	✔		

TABLE II

The present method is usable in connection with:

- registration and issuance of Electronic Security Credentials (ESC)
- real time authorization of sensitive transactions (e.g., high financial value, age sensitive material, etc.)
- collection of payment information (e.g., credit card information).

The present system and method meet a significant number of the requirements necessary for effective first-time registration and subsequent maintenance of security credentials: speed, security, scalability and a strong audit trail. In one aspect, an automated, self-service tool to aid in quickly and reliably verifying a person's identity over the Internet is provided.

In another aspect, the Public Switched Telephone Network (**PSTN**) is a factor in authentication. The system contains mechanisms that enable the synchronization of a session established over an electronic network, such as the Internet, with a session established over the Public Switched Telephone Network (a phone call).

A person's ability to answer a phone call at their own phone number behaves as a "something you have" rather than a "something you know". In the case of a telephone number, it is easy for a disreputable party to determine your phone number (as a something you know), but it is far more difficult for the disreputable party to actually gain access to your phone to receive a call on the phone (as a something you have).

There is no law against knowing your phone number (even if it is unlisted), but there are laws against unauthorized access to the telephone line which your telephone number represents. A criminal's knowledge of your phone number allows him to call it, but he cannot answer it. The present system requires simultaneous or substantially simultaneous use of the phone and a nearby computer connected to the Internet.

In addition to using the PSTN as an authentication factor, the use of the PSTN also makes it possible to use a voice recording to create an audit trail. That voice recording could also be used as input for voice biometrics (one's voiceprint is a "something you are") as an additional factor of authentication. This would be especially useful if an electronic security credential must be re-issued to a traveling (i.e., away from a known telephone number) subject.

In another aspect, the system is configured such that a site owner can request any number of voice recordings, keypad entries, and web pages together to create a customized authentication application. A scripting component of the system provides this flexibility within the various applications running on the system.

The Scripting capability enables a given transaction to be validated in a distinct way. For instance one type of transaction might only require a phone call to be placed and a confirmation number to be entered. Another type of transaction may require four voice recordings along with a keypad entry of the year the site visitor was born.

In yet another embodiment, a transaction record of an authentication session can be created. The transaction record may include, as exemplary information: site visitor information, the site owner who sent the request, the acceptance recording, the name

recording, the IP address of the site visitor, the confirmation number issued and entered, the phone number called, a trusted date/time stamp, and a digital signature of the information.

The transaction record provides a substantial evidentiary trail that the site visitor was the one who carried out the authenticating/authorizing transaction. This audit trail can also be used to allow the completion of future transactions, in the case of registration, for electronic security credential re-issuance based on voiceprint biometrics, or the human Help Desk equivalent—listening to the audit recording and comparing it to the Site visitor's voice on the phone.

This recorded audit trail may be made available to site owners via telephone, or via the Internet (using techniques such as streaming audio or audio file players). The audit trail can also be placed on a server allowing the site owner to retrieve the data at its own discretion.

It will be understood that communication between a target site and an authentication/authorization service can take place in various ways. In one form, the authentication service can accept a redirect from the target site and take control of the network session with the site visitor. Alternately, the target site can maintain control of the network session with the visitor and communicate with the authentication/ authorization service via a separate independent network session.

Numerous other advantages and features of the present invention will become readily apparent from the following detailed description of the invention and the embodiments thereof, from the claims and from the accompanying drawings in which details of the invention are fully and completely disclosed as part of this specification.

Brief Description Of The Drawings

Fig. 1 is a block diagram of a system in accordance with the present invention;

Fig. 2 is a diagram which illustrates the steps of a method in accordance with the present invention;

Fig. 3 is a block diagram of the system of Fig. 1 for implementing a registration process;

Fig. 4 is a copy of a visitor's screen displayed to initiate a registration process;

Fig. 5 is a view of a visitor's prompt screen for submitting information;

Fig. 6 is a view of a visitor's screen for submitting or selecting a phone number;

Fig. 7 is a copy of a visitor's screen querying the visitor about his/her ability to answer a telephone call simultaneously while connected to the internet;

Fig. 8 is a reconfirmation of the information provided on the screen of Fig. 7;

Fig. 9 is a copy of a visitor's screen informing the visitor that an automated call is being placed to him/her while on-line;

Fig. 10 is a view of a visitor's screen prompting the visitor to listen to an audible message presented via telephone;

Fig. 11 is a visitor's screen illustrating a final step of the registration process;

Fig. 12 is a visitor's screen reconfirming that the visitor must disconnect before answering a telephone call;

Fig. 13 is a screen which presents confirmation information to the visitor with instructions;

Fig. 14 is a visitor's screen illustrating instructions for proceeding after the telephone call has been concluded;

Fig. 15 is a screen requesting that the visitor specify how much time is needed to log off the internet;

Fig. 16 is a reconfirmation of the confirmation information previously presented on Fig. 13; and

Fig. 17 is a log-off screen prior to the telephone call being placed to the visitor.

Detailed Description Of The Invention

While this invention is susceptible of embodiment in many different forms, there are shown in the drawings and will be described herein in detail, specific embodiments thereof with the understanding that the present disclosure is to be considered as an exemplification of the principles of the invention and is not intended to limit the invention to the specific embodiments illustrated.

FIG. 1 illustrates a system 10 for carrying out an interactive, authentication/ authorization process. In one aspect, system 10 as discussed below can be implemented using a multi-line approach. Alternately, a single line approach can be used.

The system 10 includes a site visitor's display 12 and associated local computer 14. The site visitor V, via a bi-directional communication link 16 can access, forward

requests to and receive services from an internet service provider 20. The internet service provider 20 which would be coupled via bi-directional communication links 22 communicates via an electronic network 26, which could be the publicly available internet or a private intranet with a target site 30 via a bi-directional communication link 32.

In a typical transaction, the visitor V logs onto target site 30 and requests, authorization, authentication or other services alone or in combination from the site 30. In response to one or more requests from the visitor V, the site 30, via a bi-directional communication link 34 and the network 26 communicates via another link 36 with an authentication/authorization server 38.

Server 38 includes authorization/authentication software in the form of prestored executable instructions P. It also includes data bases D wherein information is stored in connection with prior transactions, or, previously supplied information provided by target site 30.

The authentication/authorization server 38 makes it possible to authenticate or authorize the site visitor V in accordance with the present invention. The server 38 receives either from target site 30 or directly from visitor V a telephone number where the visitor V can be called or reached essentially immediately.

The server 38 includes executable instructions P for implementing either a multi-line environment wherein the visitor V can communicate by telephone simultaneously while being on-line with the server 38 or a single line environment wherein the visitor V must log off so as to receive the telephone called discussed subsequently and then log back on again.

In a multi-line environment, the server 38 interacts in real time with the visitor V both via the network 26 and via the switched telephone network 44. In this circumstance, prior to the telephone call, the authentication/authorization software P transmits, via the network 26, confirmation information. This information appears on the visitor's display 12.

Confirmation information can include alphanumeric sequences of information of a type the visitor V can key in or audibly speak into a telephone 46. The server 38 then

automatically places a telephone call via the network 44 to the phone 46 using the number supplied by the site visitor V.

The server 38 can, once the visitor V has picked up the telephone 46, verbally confirm with the visitor V that it is in fact the individual who has logged onto site 30 and that that individual is in fact expecting a call at that telephone. The server 38 then verbally requests the visitor V to key or speak the confirmation information which has just been received on display 12.

The server 38 can also request that the visitor V speak into the telephone 46 for purposes of creating one or more stored voice files usable as part of an audit trail.

Assuming that the appropriate confirmation information has been fed back by the visitor V to the server 38 using the network 44, the server 38 can direct the visitor V to terminate the telephone call. The server 38 can then compare the received confirmation information to the transmitting confirmation and determine if they are the same. Control of the visitor's browser can then be returned to target site 30 along with a message confirming the identify of the visitor V or providing authorization information in connection with a transaction based on initial information stored in data base D of server 38. Either one alone or both of servers 38 and site 30 can be involved in making the authentication/authorization decision. The site 30 then continues the transaction and communicates directly with a visitor V.

It will be understood that a variety of types of confirmation information can be transmitted via server 38 to the visitor V using the out-of-band transmission link, namely the public switched telephone network 44. Similarly, a variety of responses by the visitor V to the server 38 can be forwarded to site 30, if desired, to be used to make the authentication/authorization decision.

Fig. 2 illustrates the steps of a process 100 implemented by the system 10. In a step 102, the visitor V logs onto target site 30 and in a step 104, provides preliminary identification information. In a step 106, the site 30 confirms a telephone number with the visitor V at which the visitor can be immediately reached. The site 30 then redirects the visitor along with the visitor's phone number to server 38.

In a step 108, server 38 assumes control of the visitor's browser and inquires of the visitor if a call can be placed at that phone number while the visitor is on-line. In a

multi-line environment, where the user answers "yes", the on-line session continues with the server 38 forwarding a confirmation code via network 26 which is in turn presented on display 12.

In a step 110, the server 38 places a telephone call to the provided phone number via the network 44 which should produce ringing at phone 46 which in turn is picked up by visitor V. The server 38 can then confirm that the visitor V, the call recipient, is expecting the call. The server 38 then requests that the visitor V either speaks or types the confirmation information on display 12.

In addition to analyzing the confirmation information fed back via network 44, the server 38 in a step 112 can request that the visitor V make predetermined voice statements such as reciting his or her name and then reciting an agreement to terms of a proposed transaction.

Visitors who remain on line during the call can then hang up the telephone and terminate the conversation. Visitors who had to be disconnected for purposes of making the telephone call via the network 44 are reminded to log back onto the site 30 and complete the registration step 104.

The server 38 then returns control of the visitor's browser in a step 114 to site 30. The site 30 then using its internal software determines whether the visitor V has satisfied the necessary requirements to permit the transaction to continue.

The following discussion and associated figures illustrate the flow where server 38 assists a credential issuing site 30′ in registering visitor V, see Fig. 3.

In the following scenario, Site Visitor V is an individual who has logged onto web site 30′ to apply for the Electronic Security Credential. "ESC" stands for Electronic Security Credential. "SO application" refers to the registration application software that runs at the "Site Owner's" facility 30′.

In the following tables, numbered steps in the left-most column which contain numbers in BOLD and UNDERLINED refer to interactions on the server 38′. The steps that are not in bold refer to interactions that the site visitor V is having on the site owner's system 30′.

Figures 4-17 illustrate the associated, exemplary Internet browser screens which are referenced within the Internet Session column of Table 3.

Two scenarios are represented in Table III and IV. Table III labeled "Immediate Synchronization" refers to a session where the site visitor V has an Internet connection that does not interfere with the previously discussed automated telephone call. Table IV labeled "Delayed Synchronization" refers to the site visitor V using the same telephone line for the internet connection as is to be used for receiving the authentifying telephone call.

Immediate Synchronization – Table III

Immediate synchronization occurs when the visitor V is using a different communications link for the internet connection than is being used for the automated call from the server 38, Fig. 1 or 38′, Fig. 3.

Step	Internet Session	PSTN Session	Comments
1	Site visitor V arrives at a prescribed web site 30′ to initiate the registration process. *(Fig. 4)*		
2	Site visitor enters information into the Site Owner's (SO) application as prompted by the web page and submits the information. *(Fig. 5)*		Information to be collected will be prescribed by the issuer of the ESC, and for exemplary purposes could contain identifying information such as name, address, SSN, employee number, account number, mother's maiden name, etc.
3	SO application uses information submitted by Site visitor to query a data store and determine if the information provided by the site visitor identifies an entity to which an ESC is to be issued by the system. *(Fig. 5)*		The Site Visitor information collected can be validated, reviewed for inconsistencies, and associated with an existing identity within the SO's system.

Step	Internet Session	PSTN Session	Comments
4	In one embodiment, the SO application displays a list of locations for telephone numbers maintained in the data store for the entity just identified. This list could be rendered as the location names, the entire telephone number, or a masked number (555-555-***5), and presented back to the Site visitor in a web page. The web page asks the Site visitor to identify at which of the listed locations Site visitor can be reached at this time. There are several other alternates from which the issuer of a credential could choose. These include: • Actual phone numbers may be presented (instead of location names) • The site visitor may be prompted to enter a phone number A combination of location name and last four digits of the number may be used to increase accuracy while maintaining privacy. *(Fig. 6)*		
5	Site visitor identifies the number of the telephone at which he/she can be reached, either by selecting a number or representative location name or by entering the number. This information is then submitted.. *(Fig. 6)*		This information is submitted to the Register system, server 38'. Therefore, after the site visitor selects a number and clicks submit, he/she is redirected to the Register server 38'. The site visitor will be unaware of this transfer because the web pages will look similar to the SO application

Step	Internet Session	PSTN Session	Comments
6	Server 38' presents a web page querying the site visitor about his/her ability to answer a call placed to a certain number while connected to the Internet. Example question is "Can you talk on 555-555-***5 while connected to the Internet?" *(Fig. 7)*		This question is presented to the Site Visitor in order to determine if the site visitor can receive the automated telephone call while connected to the Internet. Alternately, they have to disconnect their computer in order to receive a telephone call.
7	Server 38' then presents a web page to the site Visitor which reconfirms the decision he/she made on the previous page. If the site visitor answered "YES" to the question above then the following text would be displayed. "I can personally answer calls placed to 555-555-***5 at the same time my computer is connected to the Internet and I can read information displayed on my computer's screen while using the telephone" *(Fig. 8)*		This web page allows the site visitor to confirm that he/she can receive a telephone call while they are connected to the Internet. It also allows the site visitor to go back to the previous question if the statement that is presented to him/her is incorrect.
8	Server 38' displays a web page telling the site visitor that an automated call is being placed to them. The web page also contains a confirmation number or alphanumeric string (Conformation information) *(Fig. 9)*	Automated telephone call is placed to the prescribed number that the site visitor has requested.	At this point, Server 38' will employ a state management technique that will enable the active internet session to be coordinated with the PSTN session (telephone call). Error conditions (busy signal, switchboard, etc.) must be appropriately handled. "Appropriate" handling will be dependent upon the requirements of the owner of the credential. Examples are: • If the line is busy, fail • If the line is busy, retry after pause

Step	Internet Session	PSTN Session	Comments
9	Same web page is displayed as in step 8. *(Fig. 9)*	Once answered, Server 38′ will respond with an identifying greeting such as: "Hello, this is XYZ Corporation's automated telephone call. If you are expecting this call, press pound. Otherwise please hang-up."	The actual content of the greeting can be controlled by site 30′ or Server 38′ or both without limitation. The Server 38′ can, as an option, require a positive action to have the person who answered the phone acknowledge an identity. For the duration of the PSTN session, Server 38′ will provide the site visitor the ability to receive help at any time. If the site visitor presses the help key (* key on the telephone), the system will react per the requirements of the site owner.
10	Same web page is displayed as in step 8. *(Fig. 9)*	Server 38′ will instruct the site visitor to enter the confirmation number from the web page into the telephone: "Please enter the confirmation number displayed on your computer screen using your telephone keypad, then press pound."	Once the site visitor has entered the confirmation number from the web page into the telephone. The Server 38′ expects that whoever is using the web browser is the same person who is on the telephone call. The Server 38′ will allow the site visitor to retry the confirmation number many times. The site owner determines how many times it will allow the site visitor to enter the confirmation number.

Step	Internet Session	PSTN Session	Comments
11	When the site visitor presses the pound key, the web page changes and has the following text: "Please listen carefully to the telephone voice prompts *(Fig. 10)*	Server 38′ will instruct the site visitor to record his/her name: "For audit purposes we need to record your name. After the tone, please say your full name, then press pound."	The Server 38′ will make a name recording for audit trail information. The owner of site 30′ can determine what information should be recorded from the site visitor V. The Server 38′ will allow many recordings or no recordings as requested by the site owner. A scripting feature provides such flexibility. The Server 38′ has mechanisms that ensure that the recordings are of good quality. The Server 38′ is able to detect if a voice is loud enough and long enough to get an accurate recording. The Server 38′ can use these recordings by applying voice biometrics to them for subsequent authentications
12	The same web page as step 11 *(Fig. 10)*	Server 38′ will instruct the site visitor to record his/her acceptance of the terms an conditions: "XYZ Corporation now needs to record your acceptance of the terms and conditions from its web site. After the tone, please say 'I accept the conditions', then press pou..d."	Again, this recording is intended to be used as an audit trail mechanism. The owner of site 30′ can determine if it would like this voice recording or any additional recordings. The owner of site 30′ decides if the Server 38′ should use speech recognition to verify proper acceptance or use number entry (e.g. "Press 1 if you accept, 2 if you do not") as an alternative.
13	The site visitor is redirected back to the site 30′ application *(Fig. 10)*	The Server 38′ reads an acknowledgement of success to the site visitor: "Congratulations, you have completed your authentification. Your new userid and password are displayed on your computer screen. Good-bye.	After the site visitor has finished the process prescribed by the owner of site 30′, he/she will be redirected back to the owner of site 30′ application, thus allowing the owner of site 30′ to distribute the ESC.

Step	Internet Session	PSTN Session	Comments
14	The site owner will display on its system the next web page in its process. It could potentially give the site visitor: -userid and password -digital certificate -personal identification number -an e-mail to an e-mail box *(Fig. 11)*		The site owner will distribute the ESC that the site visitor was initially seeking when he/she came to the SO application in step 1.

Delayed Synchronization – Table IV

The delayed synchronization scenario occurs when the site visitor V is using the same telephone line for his/her Internet connection as he/she is using to receive the automated telephone call, thus forcing the site visitor to temporarily disconnect from the Internet.

Step	Internet Session	PSTN Session	Comments
1	Site visitor arrives at a prescribed web site to initiate the registration process. *(Fig. 4)*		
2	Site visitor enters information into the Site Owner's application as prompted by the web page and submits the information. *(Fig. 5)*		Information to be collected will be prescribed by the issuer of the ESC, and could contain identifying information such as name, address, SSN, employee number, account number, mother's maiden name, etc.
3	SO application uses information submitted by Site visitor to query a data store and determine if the information provided by the site visitor identifies an entity to which an ESC is to be issued by the system. *(Fig. 5)*		The Site Visitor information collected can be validated, reviewed for inconsistencies, and associated with an existing identity within the SO's system.

Step	Internet Session	PSTN Session	Comments
4	In one embodiment, the SO application displays a list of locations for telephone numbers maintained in the data store for the entity just identified. This list could be rendered as the location names, the entire telephone number, or a masked number (555-555-***5), and presented back to the Site visitor in a web page. The web page asks the Site visitor to identify at which of the listed locations Site visitor can be reached at this time. There are several other alternates from which the issuer of a credential could choose. These include: • Actual phone numbers may be presented (instad of location names) • The site visitor may be prompted to enter a phone number A combination of location name and last four digits of the number may be used to increase accuracy while maintaining privacy. *(Fig. 6)*		
5	Site visitor identifies the number of the telephone at which he/she can be reached, either by selecting a number or representative location name or by entering the number. This information is then submitted. *(Fig. 6)*		**IMPORTANT** This information is submitted to the system. Therefore, after the site visitor selects a number and clicks submit, he/she is redirected to the Server 38'. The site visitor will be unaware of this because the web pages will look similar to the SO application

Step	Internet Session	PSTN Session	Comments
6	Server 38′ presents a web page querying the site visitor about his/her ability to answer a call placed to a certain number while connected to the Internet. Example question is "Can you talk on 555-555-***5 while connected to the Internet?" *(Fig. 7)*		This question is presented to the Site Visitor in order to determine if the site visitor can receive the automated telephone call while connected to the Internet. Alternately, he/she have to disconnect their computer in order to receive a telephone call.
7	Server 38′ then presents a web page to the site visitor which reconfirms the decision he/she made on the previous page. If the site visitor answered "NO" to the question above then the following text would be displayed. "To personally answer a telephone call placed to 555-555-***5, I must first disconnect my computer from the Internet" *(Fig. 12)*		This web page allows the site visitor to confirm that he/she must disconnect the computer from the Internet in order to receive the phone call. It also allows the site visitor to go back to the previous question if the statement that is presented to him/her is incorrect.
8	Server 38′ presents a web page with a confirmation number on it. *(Fig. 13)*		The site visitor needs to write down or print out the web page in order to use the confirmation number during the telephone call.
9	Server 38′ presents a web page which contains a URL 'www.finishregistration.com' *(Fig. 14)*		The site visitor needs to remember or write down the URL because after the telephone call he/she will need to reconnect to the Internet and direct their web browser to the URL that is shown on the web page. The reason this is done is because the system must close out the site visitors session before redirecting to the site visitor back to the SO application
10	Server 38′ then presents a web page allowing the site visitor to select how long they want to wait before the call is placed to him/her. *(Fig. 15)*		The site visitor will be able to choose the delay time before the telephone call is placed. The SO will instruct as to the values that the Server 38′ will display to the site visitor.

Step	Internet Session	PSTN Session	Comments
11	Server 38′ presents a web page reminding the site visitor about the confirmation number and the URL (web address) *(Fig. 16)*		The Server 38′ reminds the site visitor one more time of the 2 pieces of information they will need to complete the authentication process.
12	Server 38′ presents a web page instructing the site visitor to disconnect from the Internet and wait for the system to place the automated telephone call *(Fig. 17)*		When the site visitor sees this screen the Server 38′ will start the timer on the time delay that was chosen in step 10. The SO decides if the Server 38′ should use speech recognition to verify proper acceptance or use number entry (e.g. "Press 1 if you accept, 2 if you do not") as an alternative. The web session is now completed, and the phone session will begin
13		Voice application begins "Hello, this is XYZ Corporation's automated telephone call. If you are expecting this call, press pound. Otherwise please hang-up."	During the phone call the site visitor is not connected to the web application. This first prompt helps identify that the Server 38′ has reached the intended party.
14		"Please enter your confirmation number, then press pound"	This step asks the site visitor to enter the number that was previously given to him/her over the web application. This ensures that the person who was on the web session is the same person that is on the telephone
15		"For audit purposes we need to record your name. After the tone, please say your full name, then press pound."	This steps takes a voice recording of the site visitor for audit purposes. The Server 38′ can use these recordings by applying voice biometrics to them for subsequent authentications.

Step	Internet Session	PSTN Session	Comments
16		"XYZ Corporation now needs to record your acceptance of the terms and conditions from its web site. After the tone, please say 'I accept the conditions', then press pound."	This step takes another voice recording of the site visitor for audit purposes. The Server 38' can use these recordings by applying voice biometrics to them for subsequent authentications.
17		"Congratulations, you have completed your telephone authorization. Please go to Internet address www.finishregistration.com to complete your registration. You must reconnect within 20 minutes to complete the process. Good-bye."	This is the last step in the phone session. After the site visitor has completed this step he/she must reconnect his/her computer to the Internet and point their web browser to 'www.finishregistration.com'. This helps reinforce the information that was given to the site visitor in steps 9 and 11. The Server 38' has the capability of requiring a site visitor to reconnect their computer and go to the appropriate web address within a certain amount of time. The amount of time is configurable as requested by the site owner.
18	Site visitor V reconnects his/her computer to the Internet and goes for example to: www.finishregistration.com *(Fig. 17)*		The Server 38' then checks which site visitor is coming back to the web site and makes all the appropriate checks to ensure he/she has indeed finished the phone session. If all the checks are successful the site visitor is redirected back to the SO application in the exact same manner as the Immediate Synchronization scenario step 13. Thus allowing the SO to distribute the ESC

Step	Internet Session	PSTN Session	Comments
19	The site owner will display on their system the next web page in their process. It could potentially give the site visitor: -userid and password -digital certificate -personal identification number -an e-mail to him/her *(Fig. 11)*		The site owner will distribute the ESC that the site visitor was initially seeking when they came to the SO application in step 1

The following is a list of sample error conditions which may occur and a suggestion of how they may be handled. Handling of many of these conditions is largely a policy issue to be decided by the owner of site 30'. Each of these failure cases has as a possible response that the electronic registration could not be completed.

	Error Condition	Possible Response
1	Busy signal	• Wait 30 seconds and call back. • Present instructions on the web to choose a different number or clear line.
2	Telephone call reaches switchboard	• Present recording requesting transfer to Site visitor. • Transfer to human agent on initiation side of the call, request transfer to Site visitor, transfer back to automated attendant. • Play the DTMF tones of the extension the system is trying to reach
4	Site visitor cancels out of web session	PSTN session thanks them for participating and terminates call.
5	Site visitor cancels out of PSTN session	Web session presents page offering alternative registration mechanisms.
6	No voice recording captured	• Provide instructions to speak more loudly. • Fail registration • Accept registration with no voice audit

Table V

From the foregoing, it will be observed that numerous variations and modifications may be effected without departing from the spirit and scope of the

invention. It is to be understood that no limitation with respect to the specific embodiment illustrated herein is intended or should be inferred. The disclosure is intended to cover the appended claims all such modifications as fall within the scope of the claims.